IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Ian RHODES

NETWORK ARRANGEMENT FOR COMMUNICATION

Serial No. 09/934,166
Appeal No.: Unknown
Group Art Unit: 2135

Enclosed is a check in the amount of Five Hundred Dollars ($500.00) to cover the official fee for this Appeal Brief. In the event that there may be any fees due with respect to the filing of this paper, please charge Deposit Account No. 50-2222.

Peter Flanagan

Peter Flanagan
Attorney for Appellant
Reg. No. 58,178

SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700

Atty. Docket: 59643.00074

PCF/kzw

Enclosures: Check No. 15132
Appeal Brief
Petition for One Month Extension of Time

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Appellant:	Confirmation No.: 8265
Ian RHODES	Appeal No.: Unknown
Serial Number: 09/934,166	Group Art Unit: 2135
Filed: August 20, 2001	Examiner: Thanhng B. TRUONG

For: NETWORK ARRANGEMENT FOR COMMUNICATION

BRIEF ON APPEAL

October 2, 2006

I. INTRODUCTION

This is an appeal from the final rejection set forth in an Official Action dated December 14, 2005, ("the Office Action") finally rejecting claims 1-24, 26-54, 56, and 59, all of the pending claims in the application. Claims 1-23, 26-54, and 56 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,548,649 of Jacobson ("Jacobson") in view of U.S. Patent No. 5,940,591 of Boyle ("Boyle"), according to the Office Action, item 3. Claims 24 and 59 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson in view of U.S. Patent No. 6,421,339 of Thomas ("Thomas"), according to the Office Action, item 4. A Response under 37 CFR 1.116 was timely filed March 14, 2006 ("the Response"). An Advisory Action maintaining the rejections was mailed March 30, 2006 ("the Advisory Action"). A Pre-Appeal Brief Request for Review, PTO/SB/33, and Notice of Appeal were timely filed, together with an appropriate petition for extension of time, on May 15, 2006 ("the PABRFR"). A Notice of Panel Decision from Pre-Appeal Brief Review was issued on August 1, 2006, indicating that claims 1-24, 26-54, 56, and 59 are still rejected and that the application remains under appeal. This Appeal Brief is being timely filed, in view of the attached petition for a one-month extension of time, within two months of the mailing date of the Notice of Panel Decision from Pre-Appeal Brief Review.

II. REAL PARTY IN INTEREST

The real party in interest in this application is Nokia Networks Oy of Espoo, Finland, by virtue of an obligation of assignment by the inventor (based on his employment) as evidenced by its designation as Appellant in the international application, PCT/GB00/00602 of which this application is a continuation application. Nokia Networks Oy, is a part of Nokia Corporation of Espoo, Finland, and thus Nokia Corporation may be considered the Real Party in Interest.

III. STATEMENT OF RELATED APPEALS AND INTERFERENCES

There are no known related appeals and/or interferences which will directly effect or be directly effected by or have a bearing on the Board's decision in this appeal.

IV. STATUS OF CLAIMS

Claims 1-24, 26-54, 56, and 59, stand rejected as being unpatentable over certain alleged prior art. The rejection of each of claims 1-24, 26-54, 56, and 59 is being appealed. Each of the appealed claims stands or falls separately, and are being argued separately and identified under a separate heading, as required by 37 C.F.R. 41.37, as can be seen in Section VIII below.

V. STATUS OF AMENDMENTS

Claims 1-24, 26-54, 56, and 59 stand as they were previously presented prior to the Office Action. No amendments have been submitted or entered since that time. Thus, claims 1-24, 26-54, 56, and 59 are pending and their respective rejections are appealed.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

The independent claims involved in this appeal are claims 1, 26-27, 37, 41-42, and 56.

Claim 1, upon which claims 2-24 and 59 depend, is directed to a method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, the first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network. *See, for example*, page 8, lines 26-40.

The method includes selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route the communication according to the information held in the storage means. *See, for example*, page 10, line 18, to page 12, line 24.

The method also includes encrypting the selectively routed communication by means of an encryption engine before it traverses the intermediate network. *See, for example*, page 12, lines 13-24.

At least one network element and the encryption engine are located substantially within the first secure network. *See, for example*, page 14, lines 15-40.

Claim 26 is directed to a method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, the first and second networks being separated by a relatively insecure network. *See, for example*, page 8, lines 26-40.

Communications from the first node to the at least one second node via the relatively insecure network are encrypted. *See, for example*, page 12, lines 13-24.

The method includes providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network. *See, for example*, page 10, line 18, to page 12, line 24.

Claim 27, upon which claims 28-36 depend, is directed to a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, the first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network. *See, for example*, page 8, lines 26-40.

The secure network arrangement includes at least one network element triggerable to refer to information held in a storage means to selectively route over the relatively insecure intermediate network or the relatively secure intermediate network a predetermined communication identified by a trigger according to the information held in the storage means from the first end terminal to the second end terminal over the relatively insecure intermediate network. *See, for example*, page 10, line 18, to page 12, line 24.

The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the intermediate network. *See, for example*, page 12, lines 13-24.

At least one network element and the encryption engine are located substantially within the first secure network. *See, for example*, page 14, lines 15-40.

Claim 37, upon which claims 38-40 depend, is directed to a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, the first and second networks being separated by at least intermediate network, wherein at least one communication route through which constitutes a relatively insecure communication route and at least one route constitutes a relatively secure communication route from the first end terminal to the second end terminal. *See, for example*, page 8, lines 26-40.

The secure network arrangement includes at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over the relatively insecure communication route or the relatively secure communication route. *See, for example*, page 10, line 18, to page 12, line 24.

The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the relatively insecure intermediate network. *See, for example*, page 12, lines 13-24.

The at least one network element and the encryption engine are located substantially within the first secure network. *See, for example*, page 14, lines 15-40.

Claim 41 is directed to a method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, the first and second networks being separated by a relatively insecure network. *See, for example*, page 8, lines 26-40.

Communications from the first node to the at least one second node via the relatively insecure network are encrypted. *See, for example*, page 12, lines 13-24.

The method includes providing at least one network element operable to store security information and being triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network. *See, for example*, page 10, line 18, to page 12, line 24.

Claim 42, upon which claims 43-54 depend, is directed to a network arrangement for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, the first and second networks being separated by a relatively insecure network. *See, for example*, page 8, lines 26-40.

Communications from the first node to the at least one second node via the relatively insecure network are encrypted. *See, for example*, page 12, lines 13-24.

The network arrangement includes at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network. *See, for example*, page 10, line 18, to page 12, line 24.

Claim 56 is directed to a network arrangement for the distribution of security information between a node in a first secure network and at least one node in a second secure network, the first and second networks being separated by a relatively insecure intermediate network. *See, for example*, page 8, lines 26-40.

The network arrangement includes, in at least one of the first and second secure networks, at least one network element operable to store security information and triggerable to distribute the security information to at least one or more target node in the second secure network. *See, for example*, page 10, line 18, to page 12, line 24.

The network arrangement also includes an encryption engine for encrypting a communication before it traverses the relatively insecure intermediate network. *See, for example*, page 12, lines 13-24.

Claim 2, which depends from claim 1, recites, in part, "wherein said at least one network element comprises switch means provided with control means and said storage means." *See, for example*, page 10, line 35, to page 10, line 16.

Claims 3-5 and 7 recite, in part, "said storage means." *See, for example*, page 10, line 35, to page 10, line 16.

Claim 6 recites "said switch means" and "the storage means." *See, for example*, page 10, line 35, to page 10, line 16.

Claims 15 and 16 recite "the storage means." *See, for example*, page 10, line 35, to page 10, line 16.

Claim 28, which depends from claim 27, recites, in part, "wherein said at least one network element comprises a switch means provided with a control means and said storage means for storing said information including routing and encryption/decryption information." *See, for example*, page 10, line 35, to page 10, line 35.

Claim 28 recites "the switch means" "the storage means" and "said storage means." *See, for example*, page 10, line 35, to page 10, line 35.

Claim 36 recites "the storage means." *See, for example*, page 10, line 35, to page 10, line 35.

Claim 38, which depends from claim 37, recites, in part, "decryption means located substantially within the second secure network." *See, for example*, page 15, lines 14-40.

Claims 39-40 recite "said decryption means." *See, for example*, page 15, lines 14-40.

Claim 44, which depends from claim 42, recites, in part, "wherein the at least one network element comprises switch means provided with control means, and storage means for storing said encryption/decryption information." *See, for example*, page 10, line 35, to page 10, line 35.

Claim 45 recites "said switch means." *See, for example*, page 10, line 35, to page 10, line 35.

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

As mentioned above, the grounds of rejection to be reviewed on appeal are as follows: the rejection of claims 1-23, 26-54, and 56 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,548,649 of Jacobson ("Jacobson") in view of U.S. Patent No. 5,940,591 of Boyle ("Boyle"), according to the Office Action, item 3; and the rejection of claims 24 and 59 under 35 U.S.C. 103(a) as being unpatentable over Jacobson in view of U.S. Patent No. 6,421,339 of Thomas ("Thomas"), according to the Office

Action, item 4.

VIII. ARGUMENT

Appellant respectfully submits that each of the pending claims, 1-24, 26-54, 56, and 59, recites subject matter that is neither disclosed nor suggested by the cited art. Each of the claims is being argued separately, and thus each of the claims stands or falls alone.

A. The Rejection of claims 1-23, 26-54, and 56 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,548,649 of Jacobson ("Jacobson") in view of U.S. Patent No. 5,940,591 of Boyle ("Boyle")

Claims 1-23, 26-54, and 56 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,548,649 of Jacobson ("Jacobson") in view of U.S. Patent No. 5,940,591 of Boyle ("Boyle"), according to the Office Action, item 3. The Office Action took the position that Jacobson teaches all the features of the claims except the distribution and/or routing of security information between the first network and the second network. The Office Action cited Boyle to remedy these particular deficiencies of Jacobson. Appellant respectfully traverses this rejection because the combination of Jacobson and Boyle does not disclose or suggest all of the elements of any of the claims.

1. Claim 1

Claim 1, upon which claims 2-24 are dependent, recites a method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by a relatively insecure intermediate network and a relatively secure intermediate network. The method includes selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route the communication according to the information held in the storage means. The method also includes encrypting the selectively routed communication by means of an encryption engine before it traverses the intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

As discussed in the specification, certain embodiments of the present invention enable subscribers to benefit from a secure network service customized according to their own preferences. First and second secure networks are separated by a relatively secure intermediate network and a relatively insecure intermediate network, and a communication is selectively routed over one of these networks. Predetermined types of communication may be selectively routed over the relatively secure intermediate network or the relatively insecure intermediate network depending on information held in the storage means. Additionally, certain embodiments of the present invention enable a network element and the encryption engine to be located substantially in the first network. Thus, encryption circuitry requirements may be reduced. It is respectfully submitted that Jacobson and Boyle, when viewed either singly or in combination, fail to disclose or suggest all the features of any of the presently pending claims. Therefore, the cited references fail to provide the critical and unobvious advantages discussed above.

The USPTO has not disputed these critical and unobvious advantages. Undisputed advantages can be the basis for claims being allowed. See, MPEP 707.07(f); *In re Herrmann*, 261 F.2d 598, 120 USPQ 182 (CCPA 1958); and *In re Soni*, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995).

Jacobson relates to a network local security bridge for bridging first and second sides of a network. Referring to Figure 1 of Jacobson, one network, Ethernet network 100, is shown having secure zones 108-1 to 108-3. A bridge 104-1 is provided for linking side 1 and side 2 of the network. Depending on the destination or source address of the packets received at bridge 104-1, the packets are filtered, and are encrypted before forwarding. Bridge 104-1 includes a number of filter tables, such as Ethernet address filter table 224-1, that are used to filter packets received dependent on the Ethernet destination address of a packet. For example, Jacobson describes first side packets as only being encrypted by the local security bridge if their destination address is within the remote secure zone, but not being encrypted if their destination address is within a remote insecure zone. Second side packets are decrypted if they originate from the remote secure zone, but not if they originate from an insecure zone. After any necessary encryption or decryption, first and second side packets are transmitted to their destination by the local security bridge.

Boyle relates to an apparatus and method for providing network security. Boyle describes a secure network interface unit (SNIU) that controls communications between a respective host or user computer unit, and a network at a session layer of interconnection. Referring to Figure 2, Boyle shows a type "a" network using labels, a type "b" network using labels, and a public network. The networks are separated by a bridge, gateway and guard, each of which forms a SNIU. A bridge SNIU is used between two private networks using the same security labeling semantics but operate at two different protection levels. The gateway SNIU is used between two networks using different security labeling semantics. A guard SNIU is used to support communication between a private network and a public network. According to Boyle, one network may use the labeling terms "top secret," "secret," "confidential," and "unclassified," while a second network can use "most secret," "secret," "restricted," "confidential," and "releasable."

Appellant submits that the combination of cited references does not disclose or suggest all the features of the pending claims. For example, Appellant submits that neither Jacobson nor Boyle discloses or suggests secure networks separated by a relatively insecure network and a relatively secure network. Jacobson describes only one network: Ethernet network 100. Claim 1 of the present application, in contrast, recites four networks (a first secure network, a second secure network, a relatively insecure intermediate network, and a relatively secure intermediate network). Further, Jacobson describes only one route being provided between one end zone and any other end zone, whether the zone is secure or insecure. Boyle also fails to disclose or suggest this feature, and therefore fails to remedy Jacobson's deficiencies. Thus, Jacobson and Boyle do not disclose or suggest first and second secure networks separated by a relatively secure intermediate network and a relatively insecure intermediate network.

The Office Action stated that Jacobson teaches these features at column 1, lines 47-64, Figure 1, and column 3, line 66, to column 4, line 7, thereof. Appellant respectfully disagrees. Neither of those passages discusses a plurality of networks, and Figure 1 clearly shows only a single network: Ethernet network 100. Indeed, reading those passages in context and with reference to Figure 1, it is apparent that only one network is disclosed.

Specifically, as can be seen at column 1, lines 44-47, and column 4, lines 11-13, the bridge between the two sections of Jacobson's network is a "local network security bridge." Thus the bridge bridges "sides 1 and 2" of the network 100. The phrase "local network" indicates that the bridge is an intranet bridge: a bridge between two parts of the same network.

Moreover, further evidence of Jacobson's teaching being limited to an intranet bridge can be seen at column 1, lines 8-43, thereof. As explained in the "Background of the

Invention" portion, Jacobson recognizes a problem for communication between hosts in **a network**. Jacobson asserts that network bridges connecting zones or segments of **a network** have been known, but that they have not been able to handle a mixture of encrypted and unencrypted traffic. Accordingly, Jacobson proposes a local network security bridge that bridges "a first side of **a network** and a second side of **the network**." (Emphasis added.) The Office Action's position that Jacobson is applicable to multiple networks is thus fundamentally flawed, because everything having to do with Jacobson's system relates to a segmented local network.

The Office Action in essence proposes *sub silentio* to modify Jacobson to apply to multiple networks. However, such a proposal would be contrary to Jacobson's intended purpose. MPEP 2143.01(V) states "THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE," (Capital letters in original.) and explains that "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." Moreover, MPEP 2145(III) states that "the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose." The proposed combination would render the primary reference, Jacobson, inoperable for its intended purpose by removing Jacobson's bridge from within the network and placing it instead at a boundary between networks, thereby preventing it from controlling the network traffic between zones or segments of a network, as it was intended.

The Office Action further responded by noting that Jacobson states, at column 1, lines 10-12, "In these types of networks, each host device is burdened with encrypting outgoing data and decrypting incoming data." Appellant respectfully submits that this comment, taken in context, supports Appellant's position. Specifically, the previous sentence states "Data encryption and decryption for secure communication between hosts in **a network** has existed for many years." (Emphasis added.) Thus, the reference to "such networks" is a reference to networks that each includes data encryption and decryption for secure communication between hosts. In other words, "such networks" is genre language for the class of networks, each of which Jacobson aims to improve.

The Office Action also responded by noting that Boyle provides, at column 4, lines 51-55 of Boyle, two private networks. Appellant respectfully submits that this disclosure is not germane to the rejection, which took the position that Jacobson taught those features. In other words, whether or not Boyle teaches two private networks does not affect the actual disclosure of Jacobson, which is a single network.

However, out of an abundance of caution, Appellant respectfully submits that the alternative rejection on the basis that it would have been obvious to modify Jacobson in view of Boyle is mistaken. It would not have been obvious to one of ordinary skill in the art to modify Jacobson's "local network security bridge" to perform security between networks (internetworking security) as opposed to security within a network (intranetworking security). As noted above, doing so would fundamentally undermine the intended purpose of Jacobson to control intranet network traffic.

Furthermore, there is no motivation to modify Jacobson on the limited basis that Boyle happens to disclose a plurality of networks. The disclosure by Boyle of a plurality of networks is not accompanied by any indication that it would be desirable to adopt a plurality of networks over a single network. Indeed, there is no disclosure in Boyle that would lead one of ordinary skill in the art to fracture Jacobson's single network into multiple networks.

Accordingly, it is respectfully submitted that the Office Action's position that Jacobson teaches that its "local network security bridge" is between two networks is fundamentally flawed, and that one of ordinary skill in the art would not have been motivated to undo the whole purpose of Jacobson to provide security within **a network** by changing the "local network security bridge" into some other kind of bridge, as the Office Action appears to have suggested.

The Advisory Action responded with two arguments, which are quite similar (if not the same) as the arguments presented by the Office Action. The Advisory Action first argued that the claim language argued and the claim language pending is not the same. The Advisory Action correctly noted that the claims call for selectively routing over "said relatively insecure intermediate network or said relatively secure intermediate network." The Advisory Action appears to have been arguing that it is not necessary for Jacobson to teach multiple networks because of the alternative language as to routing. However, one cannot selectively route over at least one of two networks unless there are at least two networks from which to select. If there is only one network, the routing is not "selective." Furthermore, Appellant respectfully notes that there is no intended difference (nor any actual difference) between the scope of "at least one of A and B" and "A or B" as explained in the Previous Response at page 17.

In this first argument, the Advisory Action accuses Appellant of using terminology "inconsistent with the accepted meaning through out [sic] the remarks." Appellant respectfully disagrees. The Advisory Action does not provide any example of any terms being used contrary to their "accepted meaning" nor does the Advisory Action attempt to define terms with regard to their "accepted meaning." In short, there is no basis for the Advisory Action's accusation.

Also, in the first argument, the Advisory Action wrongly stated "the above argument's limitation does not even support by [sic] the specification to rescue Appellant's position." There is also no basis for this accusation. The specification fully supports both the claims and the arguments in favor of patentability previously and presently presented. The Advisory Action does not point out with particularity the limitation that is supposedly not supported by the specification. However, assuming the limitation is the feature related to selectively routing, the Advisory Action is in clear factual error, because the feature is clearly supported by the specification. *See, for example,* page 11, line 31, to page 12, line

24.

The second argument of the Advisory Action is that Jacobson does teach these features, and essentially repeats the arguments of the Office Action. These arguments are fully rebutted above.

Moreover, claim 1 currently recites four networks: a first secure network, a second secure network, a relatively insecure intermediate network, and a relatively secure intermediate network.

The Office Action did not address with particularity the basis for Jacobson teaching these features. However, the Office Action specifically referred to Jacobson's figure 1 with regard to the selective routing feature, which depends for its antecedent reference on two of these four recited networks. Figure 1 of Jacobson discloses an Ethernet network 100 comprising secure zones 108-1 to 108-3. A bridge 104-1 is provided for linking two sides, side 1 and side 2, of the network. Depending on the destination or source address of packets received at bridge 104-1, the packets may be filtered, and may be encrypted before forwarding. Bridge 104-1 includes a number of filter tables, for example Ethernet address filter table 224-1 which is used to filter packets received dependent on the Ethernet destination address of a packet.

Even if secure zone 108-1, 108-2, and 108-3 were interpreted as being "secure networks," (not admitted) Jacobson fails to disclose secure networks separated by a relatively secure and a relatively insecure network (such that one or other could be selected for selective routing). As can be shown in the enclosed marked-up version of Jacobson's Figure 1, (previously submitted during prosecution) the only network that links the host units in the secure zones is the "insecure" Ethernet network 100. Furthermore, only one route is ever provided between one end zone in Jacobson and any other end zone.

In contrast, claim 1 recites first and second secure networks separated by a relatively secure intermediate network and a relatively insecure intermediate network, and a communication is selectively routed over one of these networks.

Appellant also submits that the cited references fail to disclose or suggest selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication. Further, Appellant submits that the cited references do not disclose or suggest selectively routing a packet over one of a relatively secure intermediate network and a relatively insecure intermediate network by a network element triggerable to refer to information held in a storage means. For example, as discussed above, Jacobson describes using one network with a bridge linking two sides of the network. A packet is filtered, and in some cases encrypted, according to filter tables and depending on the destination address of the packet.

Thus, the packet is filtered in Jacobson, not based on a predetermined type of communication, but rather based on its address. Accordingly, the routing of Jacobson, is not based on the communication being a "predetermined type of communication," and therefore Jacobson also does not disclose this feature of the claim.

Appellant also submits that the cited references do not disclose or suggest storage means to selectively route the communication. Instead, for example, Jacobson describes using the destination address and the filter table to route a packet. Appellant submits Boyle also does not disclose or suggest these features. Thus, Appellant submits that the cited references do not disclose or suggest at least these features of the pending claims.

The Office Action responded that the features discussed immediately above are shown in Figures 2 and 4a-4c of Jacobson. Appellant respectfully disagrees. Figure 2 is a block diagram of a network security bridge, and Figures 4a-4c are the detailed flow of operation of the same network security bridge. As explained at column 4, lines 11-13, this "network local security" bridge bridges "sides 1 and 2" of the network. Accordingly, the network local security bridge 104-1 cannot perform "selectively routing, over the relatively insecure intermediate network or the relatively secure intermediate network, a predetermined type of communication." Both because it does not discuss selectively routing with respect to alternative networks nor based on a predetermined type of communication.

The Office Action admitted that Jacobson does not "explicitly point out the distribution and/or routing of security information between the first network and the second network." Appellant submits that Boyle, either alone or in combination with Jacobson, also does not disclose or suggest the feature of routing security information. As discussed above, Boyle describes data classified as "secret" or "most secret" being distributed between networks. Boyle, however, does not disclose or suggest the distribution of security information between networks. Appellant submits that the data with a high security rating or clearance of Boyle does not disclose or suggest security information that defines security parameters. For example, security information, as claimed, may include encryption/decryption information and electronic cash bit strings. Appellant submits that Boyle fails to disclose or suggest the distribution or selectively routing of security information. Thus, Jacobson and Boyle fail to disclose or suggest at least these features of the pending claims.

Appellant notes that the arguments relating to security information as opposed to confidentiality classifications (such as secret, most secret, etc.) were unanswered and unaddressed by the Office Action and the Advisory Action. Appellant notes that the ordinary meaning of "security" in the realm of network security does not include confidentiality classifications used to classify secrets. There is nothing in the present specification that would lead one to conclude that the ordinary meaning of the term "security" has been altered by the Appellant, and therefore the accidental use of the term "security" with a different meaning in Boyle is not a proper basis for rejecting the claims.

The Advisory Action's response as to this feature appears to be a cut-and-paste of the Office Action's Response to Arguments section with the word "Thus," prefixed thereto This argument does not meaningfully respond to the arguments presented, just as it did not meaningfully respond to the arguments previously presented. The USPTO cannot ignore the plain meaning of the term "security" as it would be understood in light of the specification in order to creatively reject the claims.

Thus, Appellant submits that the cited references do not disclose or suggest "selectively routing, over said relatively insecure intermediate network or said relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means," as recited in claim 1.

Moreover, the combination of Jacobson and Boyle is improper hindsight combination. The Office Action began with the template of the claims and tried to reconstruct the invention within that template. To protect against such invalid and inappropriate hindsight reconstruction, the Federal Circuit has ruled that references cannot be selected, and selected elements from selected references cannot be combined, without some suggestion, motivation, or teaching that would render obvious that selection and that combination. *See, e.g., Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1385, 58 USPQ2d 1286, 1293 (Fed. Cir. 2001) ("In holding an invention obvious in view of a combination of references, there must be some suggestion, motivation, or teaching in the prior art that would have led a person of ordinary skill in the art to select the references and combine them in the way that would produce the claimed invention."); and *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25 (Fed. Cir. 2000) ("a showing of a suggestion, teaching, or motivation to combine the prior art references is an 'essential component of an obviousness holding'").

The Office Action asserted that it would have been obvious to combine the references "since it would be highly desirable to provide multi-level security in a non-secure environment, i.e. where both the network and the hosts are not trusted, so that existing hosts and network assets would not have to be replaced by trusted hosts or secure network assets. It is also required that such an MLS system must provide user accountability and data integrity during all phases of operation within the network." The Office Action cited column 2, lines 35-41, which the Office Action was quoting word-for-word. Appellants thus respectfully traverse the Office Action's assertion of motivation to combine the references, because it is not based on any reasonable analysis.

Even taking Boyle's assertions at face value, the Office Action does not establish or even assert that Jacobson's system is a non-secure environment, i.e. where both the network and the hosts are not trusted. Accordingly, Boyle's assertion is relevant only to the implementation of Boyle in such situations, but Jacobson's system is not such a system, and thus there is no teaching, motivation, or suggestion to combine Boyle with Jacobson with Boyle.

Thus, it can be seen that Boyle was selected for combination with Jacobson by the Office Action based on the disclosure of the present application, not based on the teaching of the art. Using the present application as the basis for combination, however, is improper hindsight reconstruction. Accordingly, for this additional reason, it is respectfully requested that the rejection of claim 1.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 1 and indicate claim 1 as allowable.

2. Claim 2

Claim 2 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 2 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 2 and indicate claim 2 as allowable.

3. Claim 3

Claim 3 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 3 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 3 and indicate claim 3 as allowable.

4. Claim 4

Claim 4 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 4 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 4 and indicate claim 4 as allowable.

5. Claim 5

Claim 5 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 5 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 5 and indicate claim 5 as allowable.

6. Claim 6

Claim 6 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 6 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 6 and indicate claim 6 as allowable.

7. Claim 7

Claim 7 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 7 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 7 and indicate claim 7 as allowable.

8. Claim 8

Claim 8 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 8 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 8 and indicate claim 8 as allowable.

9. Claim 9

Claim 9 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 9 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board

reverse the rejection of claim 9 and indicate claim 9 as allowable.

10. Claim 10

Claim 10 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 10 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 10 and indicate claim 10 as allowable.

11. Claim 11

Claim 11 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 11 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 11 and indicate claim 11 as allowable.

12. Claim 12

Claim 12 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 12 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 12 and indicate claim 12 as allowable.

13. Claim 13

Claim 13 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 13 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 13 and indicate claim 13 as allowable.

14. Claim 14

Claim 14 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 14 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 14 and indicate claim 14 as allowable.

15. Claim 15

Claim 15 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 15 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 15 and indicate claim 15 as allowable.

16. Claim 16

Claim 16 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 16 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 16 and indicate claim 16 as allowable.

17. Claim 17

Claim 17 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 17 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 17 and indicate claim 17 as allowable.

18. Claim 18

Claim 18 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 18 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 18 and indicate claim 18 as allowable.

19. Claim 19

Claim 19 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 19 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 19 and indicate claim 19 as allowable.

20. Claim 20

Claim 20 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 20 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 20 and indicate claim 20 as allowable.

21. Claim 21

Claim 21 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 21 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 21 and indicate claim 21 as allowable.

22. Claim 22

Claim 22 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 22 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 22 and indicate claim 22 as allowable.

23. Claim 23

Claim 23 depends from claim 1 and recites additional limitations. Accordingly, it is respectfully submitted that claim 23 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 23 and indicate claim 23 as allowable.

24. Claim 26

Claim 26 recites a method for the distribution of security information between a first node in a first secure network and at least one node in a second secure network. The first and the second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The method includes the step of providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Accordingly, although claim 26 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 26. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network" as recited by claim 26.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 26 and indicate claim 26 as allowable.

25. Claim 27

Claim 27, upon which claims 28-36 are dependent, recites a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by a relatively insecure intermediate network and a relatively secure intermediate network. The secure network arrangement includes at least one network element triggerable to refer to information held in a storage means to selectively route over the relatively insecure intermediate network or the relatively secure intermediate network a predetermined communication identified by a trigger according to the information held in the storage means from the first end terminal to the second end terminal. The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Accordingly, although claim 27 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 27. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "at least one network element triggerable to refer to information held in a storage means to selectively route over said relatively insecure intermediate network or said relatively secure intermediate network a predetermined communication identified by a trigger according to said information held in said storage means from the first end terminal to the second end terminal over said relatively insecure intermediate network" as recited by claim 27.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 27 and indicate claim 27 as allowable.

26. Claim 28

Claim 28 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 28 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 28 and indicate claim 28 as allowable.

27. Claim 29

Claim 29 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 29 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 29 and indicate claim 29 as allowable.

28. Claim 30

Claim 30 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 30 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 30 and indicate claim 30 as allowable.

29. Claim 31

Claim 31 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 31 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 31 and indicate claim 31 as allowable.

30. Claim 32

Claim 32 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 32 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 32 and indicate claim 32 as allowable.

31. Claim 33

Claim 33 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 33 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 33 and indicate claim 33 as allowable.

32. Claim 34

Claim 34 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 34 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 34 and indicate claim 34 as allowable.

33. Claim 35

Claim 35 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 35 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board

reverse the rejection of claim 35 and indicate claim 35 as allowable.

34. Claim 36

Claim 36 depends from claim 27 and recites additional limitations. Accordingly, it is respectfully submitted that claim 36 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 36 and indicate claim 36 as allowable.

35. Claim 37

Claim 37, upon which claims 38-40 are dependent, recites a secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by at least one intermediate network. At least one communication route constitutes a relatively insecure communication route and at least one route constitutes a relatively secure communication route from the first end terminal to the second end terminal. The secure network arrangement includes at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over the relatively insecure communication route or the relatively secure communication route. The secure network arrangement also includes an encryption engine for encrypting the selectively routed communication before it traverses the relatively insecure intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Accordingly, although claim 37 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 37. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "said first and second networks being separated by at least intermediate network, wherein at least one communication route through which constitutes a relatively insecure communication route and at least one route constitutes a relatively secure communication route from the first end terminal to the second end terminal, the secure network arrangement including at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over said relatively insecure communication route or said relatively secure communication route" as recited by claim 37.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 37 and indicate claim 37 as allowable.

36. Claim 38

Claim 38 depends from claim 37 and recites additional limitations. Accordingly, it is respectfully submitted that claim 38 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 38 and indicate claim 38 as allowable.

37. Claim 39

Claim 39 depends from claim 37 and recites additional limitations. Accordingly, it is respectfully submitted that claim 39 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 39 and indicate claim 39 as allowable.

38. Claim 40

Claim 40 depends from claim 37 and recites additional limitations. Accordingly, it is respectfully submitted that claim 40 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 40 and indicate claim 40 as allowable.

39. Claim 41

Claim 41 recites a method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network. The first and second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The method includes providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Accordingly, although claim 41 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 41. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network" as recited by claim 41.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 41 and indicate claim 41 as allowable.

40. Claim 42

Claims 42, upon which claims 43-54 are dependent, recites a network arrangement for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network. The first and second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted. The network arrangement includes at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Accordingly, although claim 42 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 42. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network" as recited by claim 42.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 42 and indicate claim 42 as allowable.

41. Claim 43

Claim 43 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 43 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 43 and indicate claim 43 as allowable.

42. Claim 44

Claim 44 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 44 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 44 and indicate claim 44 as allowable.

43. Claim 45

Claim 45 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 45 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 45 and indicate claim 45 as allowable.

44. Claim 46

Claim 46 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 46 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 46 and indicate claim 46 as allowable.

45. Claim 47

Claim 47 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 47 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 47 and indicate claim 47 as allowable.

46. Claim 48

Claim 48 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 48 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 48 and indicate claim 48 as allowable.

47. Claim 49

Claim 49 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 49 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board

reverse the rejection of claim 49 and indicate claim 49 as allowable.

48. Claim 50

Claim 50 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 50 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 50 and indicate claim 50 as allowable.

49. Claim 51

Claim 51 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 51 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 51 and indicate claim 51 as allowable.

50. Claim 52

Claim 52 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 52 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 52 and indicate claim 52 as allowable.

51. Claim 53

Claim 53 depends from claim 42 and recites additional limitations. Accordingly, it is respectfully submitted that claim 53 recites features that are neither disclosed nor suggested by the combination of Jacobson and Boyle, even if it were proper, which it is not.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 53 and indicate claim 53 as allowable.

52. Claim 54

53. Claim 56

Claim 56 recites a network arrangement for the distribution of security between a node in a first secure network and at least one node in a second secure network. The first and second networks are separated by a relatively insecure intermediate network. The network arrangement includes, in at least one of the first and second secure networks, at least one network element operable to store security information and triggerable to distribute the security information to at least one target node in the second secure network. The network arrangement also includes an encryption engine for encrypting a communication before it traverses the relatively insecure intermediate network.

Accordingly, although claim 56 has its own scope, the arguments above, as to the patentability of claim 1 are also sufficient to rebut the rejection of claim 56. The combination of Jacobson and Boyle, even if proper (which it is not) would not disclose or suggest, "distribution of security information between a node in a first secure network and at least one node in a second secure network, said first and second networks being separated by a relatively insecure intermediate network" as recited by claim 56.

Thus, for all the reasons explained above, it is respectfully requested that the Board reverse the rejection of claim 56 and indicate claim 56 as allowable.

B. The Rejection of claims 24 and 59 under 35 U.S.C. 103(a) as being unpatentable over Jacobson in view of U.S. Patent No. 6,421,339 of Thomas ("Thomas").

Claims 24 and 59 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson in view of U.S. Patent No. 6,421,339 of Thomas ("Thomas"), according to the Office Action, item 4. The Office Action took the position that Jacobson does not teach providing the routing and/or access point to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network. The Office Action then took the position that Thomas taught those features of the claims missing from Jacobson. Appellant respectfully traverses this rejection because the combination of Jacobson and Thomas fails to disclose or suggest all of the elements of any of the presently pending claims.

1. Claim 24

Claim 24 depends directly from claim 1. Claim 1 is summarized above. Appellant submits that claim 24 recites the features of claim 1, and also recites the features of the selectively routing step including providing the routing to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

The deficiencies of Jacobson with respect to claim 1 are noted above, and some of the deficiencies of Jacobson with regard to claim 1 are admitted by the Office Action in the rejection of claim 1. Thomas does not remedy the above-identified deficiencies of Jacobson. The Office Action did not include Boyle in the rejection of claim 24. However, as noted above, the combination of Jacobson and Boyle is still deficient as to claim 1. Thomas also does not remedy the joint deficiencies of Jacobson and Boyle.

Thomas relates to methods and systems for call-forwarding. Thomas describes a compliant data packet network with a registering function whereby home-based users are identified separate from visiting users having other networks as home bases. The user location data of Thomas may be retrieved and modified as those users roam to other compliant networks and register with a gatekeeper at that visited network. The registration of a visiting user with a visited gatekeeper includes the process of assigning a transient identity to the roaming user, obtaining confirmation from the home gatekeeper that roaming is authorized when registering the roaming user's present address and transient identity at the home site so that calls received at the home network can be directed to the user at the visited site.

Appellant submits that Jacobson and Thomas, either alone or in combination, do not disclose or suggest selectively routing, over one of the relatively insecure intermediate network and the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means. Thomas describes home-based users being identified separate from visiting users having other networks as home bases. Thomas does not disclose or suggest selectively routing a predetermined type of communication over a relatively insecure intermediate network by means of one or more network elements according to information in a storage means. Therefore, Appellant submits that Thomas, either alone or in combination with Jacobson, does not disclose or suggest all the features of the pending claims.

Further, claim 24 is directly or indirectly dependent upon independent claim 1. If an independent claim is nonobvious, then any claim depending therefrom also is nonobvious.

MPEP 2143.03. Because independent claim 1 is nonobvious over the cited references, claim 24 is also are nonobvious. Thus, claim 24 is not rendered obvious by the cited references and Appellant respectfully requests that the obviousness rejection be withdrawn.

Moreover, the combination of Jacobson and Thomas is improper hindsight combination. The Office Action began with the template of claim 24 and tried to reconstruct the invention within that template. To protect against such invalid and inappropriate hindsight reconstruction, the Federal Circuit has ruled that references cannot be selected, and selected elements from selected references cannot be combined, without some suggestion, motivation, or teaching that would render obvious that selection and that combination. *See, e.g., Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1385, 58 USPQ2d 1286, 1293 (Fed. Cir. 2001) ("In holding an invention obvious in view of a combination of references, there must be some suggestion, motivation, or teaching in the prior art that would have led a person of ordinary skill in the art to select the references and combine them in the way that would produce the claimed invention."); and *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25 (Fed. Cir. 2000) ("a showing of a suggestion, teaching, or motivation to combine the prior art references is an 'essential component of an obviousness holding'").

The Office Action asserted that it would have been obvious to combine the references "for accommodating roaming endpoint users across H.232 compliant data network domains," citing column 1, lines 6-8 of Thomas. Appellant respectfully traverses the Office Action's assertion of motivation to combine the references, because it is not based on a reasonable analysis of the evidence. There is no indication in Jacobson that there are roaming endpoint users – or that there would be any need to accommodate them. Accordingly, even if Thomas is useful for "accommodating roaming endpoint users across H.232 compliant data network domains" that use does not provide motivation to combine the teachings of Thomas with the teachings of Jacobson. Virtually every published patent will indicate that the disclosure therein has some use, but that is not motivation to combine any patent with any other patent as necessary to reject claims.

The only reason that the Office Action combined Jacobson and Thomas was the disclosure of the present application. Using the present application as the basis for combination, however, is improper hindsight reconstruction. Accordingly, for this additional reason, it is respectfully requested that the rejection of claim 24 be withdrawn.

2. Claim 59

Claim 59 depends indirectly from claim 1. Appellant submits that claim 59 recites the features of claim 1, and also recites the features of the providing step including providing the access point to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

The deficiencies of Jacobson with respect to claim 1 are noted above, and some of the deficiencies of Jacobson with regard to claim 1 are admitted by the Office Action in the rejection of claim 1. Thomas does not remedy the above-identified deficiencies of Jacobson. The Office Action did not include Boyle in the rejection of claim 59. However, as noted above, the combination of Jacobson and Boyle is still deficient as to claim 1. Thomas also does not remedy the joint deficiencies of Jacobson and Boyle.

Thomas is discussed above. Appellant submits that Jacobson and Thomas, either alone or in combination, do not disclose or suggest selectively routing, over one of the relatively insecure intermediate network and the relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means.

Therefore, Appellant submits that Thomas, either alone or in combination with Jacobson, does not disclose or suggest all the features of any of the presently pending claims.

Further, claim 59 is directly or indirectly dependent upon independent claim 1. If an independent claim is nonobvious, then any claim depending therefrom also is nonobvious. MPEP 2143.03. Because independent claim 1 is nonobvious over the cited references, claim 59 also is nonobvious. Thus, claim 59 is not rendered obvious by the cited references and Appellant respectfully requests that the obviousness rejection be withdrawn.

Moreover, the combination of Jacobson and Thomas is improper hindsight combination. The Office Action began with the template of claim 59 and tried to reconstruct the invention within that template. To protect against such invalid and inappropriate hindsight reconstruction, the Federal Circuit has ruled that references cannot be selected, and selected elements from selected references cannot be combined, without some suggestion, motivation, or teaching that would render obvious that selection and that combination. *See, e.g., Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1385, 58 USPQ2d 1286, 1293 (Fed. Cir. 2001) ("In holding an invention obvious in view of a combination of references, there must be some suggestion, motivation, or teaching in the prior art that would have led a person of ordinary skill in the art to select the references and combine them in the way that would produce the claimed invention."); and *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25 (Fed. Cir. 2000) ("a showing of a suggestion, teaching, or motivation to combine the prior art references is an 'essential component of an obviousness holding'").

The Office Action asserted that it would have been obvious to combine the references "for accommodating roaming endpoint users across H.232 compliant data network domains," citing column 1, lines 6-8 of Thomas. Appellant respectfully traverses the Office Action's assertion of motivation to combine the references, because it is not based on a reasonable analysis of the evidence. There is no indication in Jacobson that there are roaming endpoint users – or that there would be any need to accommodate them. Accordingly, even if Thomas is useful for "accommodating roaming endpoint users across

H.232 compliant data network domains" that use does not provide motivation to combine the teachings of Thomas with the teachings of Jacobson. Virtually every published patent will indicate that the disclosure therein has some use, but that is not motivation to combine any patent with any other patent as necessary to reject claims.

The only reason that the Office Action combined Jacobson and Thomas was the disclosure of the present application. Using the present application as the basis for combination, however, is improper hindsight reconstruction. Accordingly, for this additional reason, it is respectfully requested that the rejection of claim 59 be withdrawn.

IX. CONCLUSION

As explained above, each of claims 1-24, 26-54, 56, and 59 recites one or more elements or features that are neither disclosed nor suggested in the cited references.

As noted above, the Office Action's analysis of Jacobson and Boyle is flawed, and its responses to Appellant's arguments amount to mere assertions that the Office Action is correct.

This final rejection being in error, therefore, Appellant respectfully requests that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the allowability of application claims 1-24, 26-54, 56, and 59.

In the event that this paper is not being timely filed, the Appellant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees which may be due with respect to this paper may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

SQUIRE, SANDERS & DEMPSEY LLP

Peter F Flanagan

Peter Flanagan
Attorney for Appellant/ Appellant
Registration No. 58,178

Atty. Docket No.: 59643.00074

8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700
Tel: (703) 720-7800
Fax (703) 720-7802

PCF:kzw

Enclosures: Appendix 1: Claims Appendix
Appendix 2: Evidence Appendix
Appendix 3: Related Proceedings Appendix
Marked-up copy of Figure 1 of Boyle

APPENDIX 1

CLAIMS APPENDIX

1. (Previously Presented) A method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network, the method including the steps of:

selectively routing, over said relatively insecure intermediate network or said relatively secure intermediate network, a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route said communication according to said information held in said storage means; and

encrypting said selectively routed communication by means of an encryption engine before it traverses said intermediate network,

wherein said at least one network element and said encryption engine are located substantially within said first secure network.

2. (Previously Presented) A method as in claim 1, wherein said at least one network

element comprises switch means provided with control means and said storage means.

3. (Previously Presented) A method as in claim 2, wherein said storage means is operable to store said information comprising routing information.

4. (Previously Presented) A method as in claim 2 or 3, wherein said storage means is operable to store said information comprising security information.

5. (Previously Presented) A method as in claim 2, wherein said storage means is operable to store said information comprising security information including at least one of the following: encryption information; decryption information; security key information; and electronic cash information.

6. (Previously Presented) A method as in claim 3, wherein said switch means is operable to selectively route the predetermined type of communication according to routing information in said information held in the storage means.

7. (Previously Presented) A method as in claim 4, wherein said encryption engine is operable to encrypt said predetermined type of communication according to security information in said information held in said storage means.

8. (Previously Presented) A method as in claim 6, comprising the step of identifying said predetermined type of communication by means of at least one of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics.

9. (Previously Presented) A method as in claim 8, wherein said predetermined type of communication is identified by means of originating and/or destination addresses.

10. (Previously Presented) A method as in claim 8, wherein said predetermined type of communication is identified by means of originating and/or destination identification numbers.

11. (Previously Presented) A method as in claim 4, wherein said storage means is operable to store said information comprising security information, said security information being distributed from a first node to at least one target node responsive to a predetermined trigger.

12. (Previously Presented) A method as in claim 3, wherein the stored routing information includes subscriber routing preferences.

13. (Previously Presented) A method as in claim 4, wherein the security information includes subscriber security preferences.

14. (Previously Presented) A method as in claim 4, wherein the security information includes encryption/decryption information defining a preferred algorithm or key for use with predetermined types of communication.

15. (Previously Presented) A method as in claim 2, wherein said information stored in the storage means is arranged to identify at least one group of users whose communications are to be routed and encrypted according to common preferences.

16. (Previously Presented) A method as in claim 2, further comprising providing a service management access point for accessing and changing said information held in the storage means.

17. (Previously Presented) A method as in claim 11, wherein said security information comprises decryption information, a distribution of said decryption information being triggered according to a predetermined schedule.

18. (Previously Presented) A method as in claim 11, wherein said security information is distributed to a node within at least one of the first and second secure networks.

19. (Previously Presented) A method as in claim 11, wherein said security information is distributed to an end terminal for the communication in question.

20. (Previously Presented) A method as in claim 11, wherein the at least one network element distributes said security information from a location substantially within the first secure network.

21. (Previously Presented) A method as in claim 11, wherein at least one network element distributes said security information from a location substantially within the second secure network.

22. (Previously Presented) A method as in claim 21, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route operated by trusted network operators.

23. (Previously Presented) A method as in claim 21, wherein said security

information is transferred to the at least one network element located in the second secure network by means of a secure communication route over said relatively insecure intermediate network.

24. (Previously Presented) A method according to claim 1, wherein said selectively routing step comprises providing said routing to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

25. (Canceled)

26. (Previously Presented) A method for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, including the step of providing at least one network element operable to store security information and triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

27. (Previously Presented) A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by a relatively insecure intermediate network and a relatively secure intermediate network, the secure network arrangement including:

at least one network element triggerable to refer to information held in a storage means to selectively route over said relatively insecure intermediate network or said relatively secure intermediate network a predetermined communication identified by a trigger according to said information held in said storage means from the first end terminal to the second end terminal over said relatively insecure intermediate network; and

an encryption engine for encrypting said selectively routed communication before it traverses said intermediate network,

wherein said at least one network element and said encryption engine are located substantially within said first secure network.

28. (Previously Presented) A secure network arrangement according to claim 27, wherein said at least one network element comprises a switch means provided with a control means and said storage means for storing said information including routing and encryption/decryption information.

29. (Previously Presented) A secure network arrangement according to claim 28, wherein the switch means is operable to selectively route said predetermined communication according to routing information held in the storage means and the encryption engine is operable to encrypt said selectively routed communication according to encryption information held in said storage means.

30. (Previously Presented) A secure network arrangement according to claim 29, wherein said predetermined communication is identified by means of at least one of the following: originating subscriber characteristics; destination subscriber characteristics; payload characteristics and network service characteristics.

31. (Previously Presented) A secure network arrangement according to claim 30, wherein said predetermined communication is identified by means of an originating or destination address.

32. (Previously Presented) A secure network arrangement according to claim 31, wherein said predetermined communication is identified by means of originating identification or destination numbers.

33. (Original) A secure network arrangement according to claim 31, wherein the

routing information and encryption/decryption information specifies operations according to subscriber preferences.

34. (Previously Presented) A secure network arrangement according to claim 33, wherein the encryption/decryption information defines a preferred algorithm or key for use with said predetermined communication.

35. (Previously Presented) A secure network arrangement according to claim 34, wherein the information held in the storage means identifies at least one group of users whose communications are to be routed and encrypted according to common preferences.

36. (Previously Presented) A secure network arrangement according to claim 27, comprising a service management access point for accessing and changing the information held in the storage means.

37. (Previously Presented) A secure network arrangement for communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network, said first and second networks being separated by at least intermediate network, wherein at least one communication route through which constitutes a relatively insecure communication route and at least one route constitutes a

relatively secure communication route from the first end terminal to the second end terminal, the secure network arrangement including at least one network element triggerable to selectively route a communication from the first end terminal to the second end terminal over said relatively insecure communication route or said relatively secure communication route; and

an encryption engine for encrypting said selectively routed communication before it traverses said relatively insecure intermediate network, wherein said at least one network element and said encryption engine are located substantially within said first secure network.

38. (Previously Presented) A secure network arrangement according to claim 37, including decryption means located substantially within the second secure network.

39. (Original) A secure network arrangement according to claim 38, wherein said decryption means are provided at the second end terminal.

40. (Original) A secure network arrangement according to claim 38, wherein said decryption means are provided at a node other than the second end terminal.

41. (Previously Presented) A method for the distribution of security information

between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, the method comprising providing at least one network element operable to store security information and being triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

42. (Previously Presented) A network arrangement for the distribution of security information between a first node in a first secure network and at least one second node in a second secure network, said first and second networks being separated by a relatively insecure network, wherein communications from said first node to the at least one second node via said relatively insecure network are encrypted, the network arrangement comprising at least one network element operable to store security information and triggerable to distribute said security information in a secure manner from said first node to at least one target node in said second secure network.

43. (Previously Presented) A network arrangement according to claim 42, wherein said network arrangement is operable to distribute said security information including at least one of encryption algorithms; decryption algorithms; security keys; and electronic

cash bit strings.

44. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element comprises switch means provided with control means, and storage means for storing said encryption/decryption information.

45. (Previously Presented) A network arrangement according to claim 42, wherein said switch means is operable to selectively distribute said security information in response to a predetermined type of communication.

46. (Original) A network arrangement according to claim 45, wherein said predetermined type of communication is identified by means of originating subscriber characteristics, destination subscriber characteristics, payload characteristics or network service characteristics.

47. (Previously Presented) A network arrangement according to claim 42, wherein said distribution is triggered according to a predetermined schedule.

48. (Previously Presented) A network arrangement according to claim 42, comprising a service management access point.

49. (Previously Presented) A network arrangement according to claim 42, wherein the security information is distributed to a node within at least one of the first secure network and second secure network, rather than a destination end terminal for the communication in question.

50. (Previously Presented) A network arrangement according to claim 42, wherein the security information is distributed to an end terminal for the communication in question.

51. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element distributes said security information from a location substantially within the first secure network.

52. (Previously Presented) A network arrangement according to claim 42, wherein the at least one network element distributes the security information from a location substantially within at least one of the first or second networks.

53. (Previously Presented) A network arrangement according to claim 52, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route operated by trusted

network operators.

54. (Previously Presented) A network arrangement according to claim 53, wherein said security information is transferred to the at least one network element located in the second secure network by means of a secure communication route over the relatively insecure intermediate network.

55. (Canceled).

56. (Previously Presented) A network arrangement for the distribution of security information between a node in a first secure network and at least one node in a second secure network, said first and second networks being separated by a relatively insecure intermediate network, including:

in at least one of said first and second secure networks, at least one network element operable to store security information and triggerable to distribute said security information to at least one or more target node in said second secure network; and

an encryption engine for encrypting a communication before it traverses said relatively insecure intermediate network.

57-58. (Canceled)

59. (Previously Presented) A method according to claim 16, wherein said providing comprises providing said access point to a subscriber in a visited network by virtue of a roaming agreement between an operator of the visited network and an operator of the subscriber's home network.

APPENDIX 2

EVIDENCE APPENDIX

No evidence under section 37 CFR 1.130, 1.131, or 1.132 has been entered or will be relied on by Appellant in this appeal.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

No decisions of the Board or of any court have been identified under 37 CFR 41.37(c)(1)(ii).

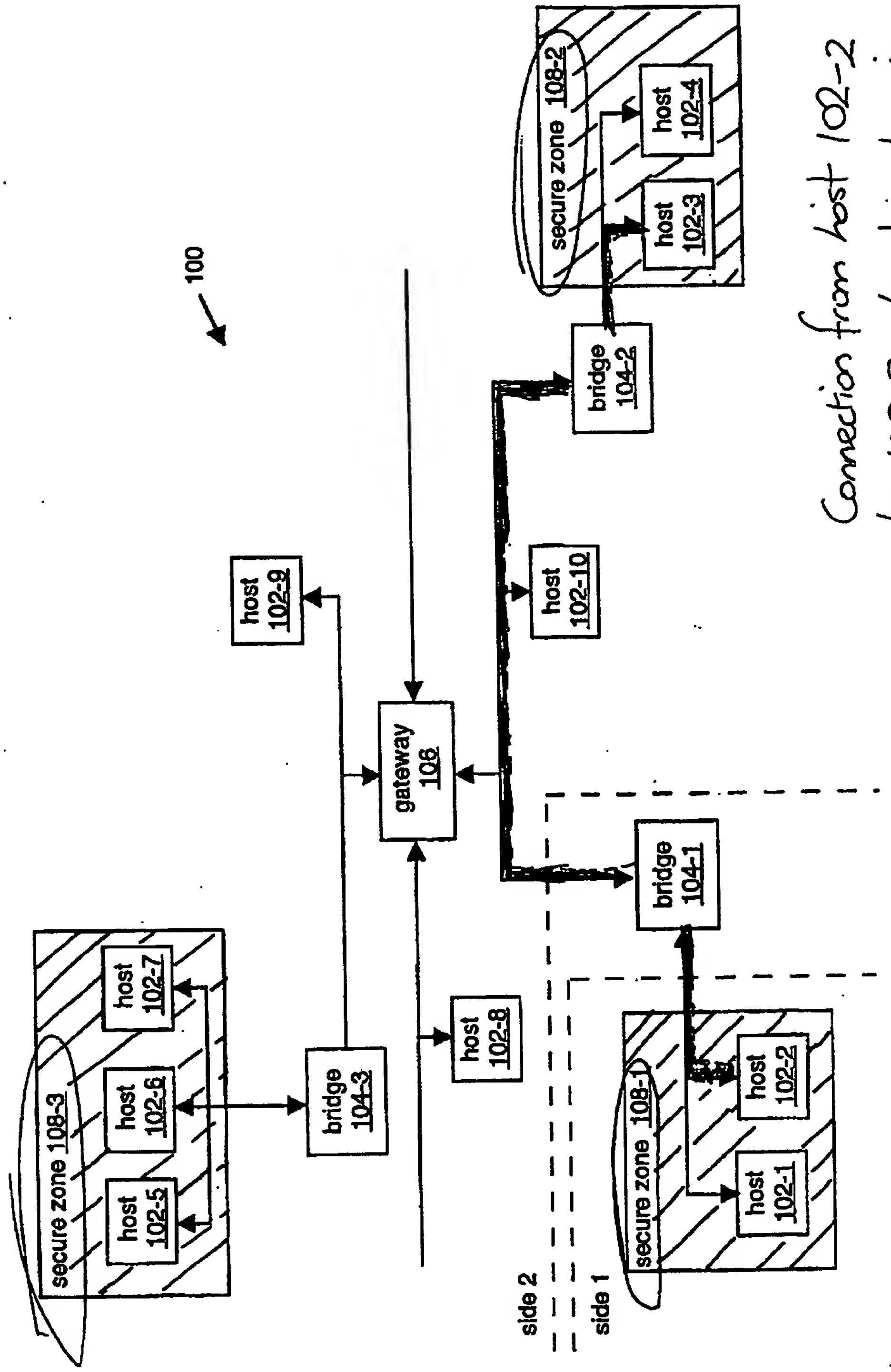

Figure 1

Connection from host 102-2 to 102-3 - travels only via relatively insecure network ie between bridge 104-1 & bridge 104-2.